AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A node of a network for managing an intrusion protection system, the node comprising:

a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

2. (Currently Amended) The node according to claim 1, wherein the ~~network exploit rule further~~ at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.

3. (Original) The node according to claim 1, wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network.

4. (Original) The node according to claim 1, further comprising a database, the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database.

5. (Original)The node according to claim 2, further comprising a machine-readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files, the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network.

6. (Original)The node according to claim 5, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

7.   (Original) The node according to claim 5, wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold.

8.   (Original) A method of distributing command and security updates in a network having an intrusion protection system, comprising:

generating a text-file defining a network-exploit rule; and

specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.

9.   (Original) The method according to claim 8, further comprising storing a plurality of text-files in a database, each text-file defining a network-exploit rule.

10.   (Original) The method according to claim 9, further comprising transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network.

11.   (Original) The method according to claim 10, wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted.

12.   (Original) The method according to claim 10, further comprising specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold.

13.   (Currently Amended) A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer;

compiling the input into a machine-readable signature file comprising machine-readable logic representative of [[the]] a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field;

evaluating the machine-readable signature file; and

determining the value of the at least one field of the machine-readable signature file.

14.   (Original) The computer readable medium according to claim 13, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value.

15.   (Original) The computer readable medium according to claim 14, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold.

16.   (Original) The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of generating a text-file from the input, the text-file specifying the network-exploit rule and the at least one field, the machine-readable signature file compiled from the text file.

17.   (Original) The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted.

18.   (New) The node according to claim 1 wherein the intrusion protection system management application is further operable to determine, based at least in part on the at least

one field, ones of a plurality of other nodes to which the network-exploit rule is to be distributed.

19.   (New) The method according to claim 8 wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule.

20.   (New) The method according to claim 8 further comprising:

distributing the network-exploit rule and the at least one field to a plurality of nodes; and

determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node.